Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1652 12/26/14

~ N. Korea Didn’t Do Hack? ~ People Are Talking! ~ EasyMiNT Update News!

~ Stuck in Your New Game? ~ Apple Automated Update ~ HP OS: The Machine!

~ Facebook Can’t Avoid Suit ~ Worst Spammers of 2014 ~ Worst Games of 2014!
~ Threats on Social Media! ~ Online Privacy Fantasy ~ Dangerous NTP Hole!

-* Happy 35th B-Day, Gaming PC! *-
-* Lizard Squad Now Tied to Sony Hack! *-
-* N. Korea’s Internet Goes Dark After Hack! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""

Well, the holiday season is winding down, with New Year’s Eve less than a week away! All of us here at A-ONE hope that you had a great holiday, spent with friends and family. We spent a fairly quiet day with the in-laws - a good distraction away from home. We didn’t take the canine "kids" with us, but made up for it with some extra treats from Santa!

So, now it’s time to erst up from the hustle and bustle of the holidays, and time to "prepare" for the New Year! We all hope that you have a great New Year’s Eve, and a healthy and prosperous new year! Happy New Year, 2015!

Until next year...

=~=~=~=

EasyMiNT Update

Hi folks,

Another EasyMiNT beta version is coming to town, hohoho.;-)

Whats new
- video mode changed in XAAES.CNF (please test this)
- APP and PRG must not be in separate folders
- added XAAES.INF
- no more networkcard driver selection on firebee, it’s installed automatically
- vincent’s e2fsck added
- bugfix: fscheck.sh

Two caveats, filesystemcheck is always invoked on firebee, seems a firebee bug and MINT folder is not backuped in firebee because MINT folder can’t be renamed under some circumstances.

Download: http://atari.st-katharina-apotheke.de/download/em190b3.zip

Substitute the old files with the files from the zip above.

Have fun!

maanke

=~=~=~=

->In This Week's Gaming Section - Lizard Squad, Hacker Group Now Tied to Sony Hack
""""""""""""""""""""""""""""""""" Microsoft Xbox Live Back Up, PS Network Still Down

Happy 35th Birthday, Gaming PC!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

This Is Lizard Squad, The Nebulous Hacker Group Now Tied to The Sony Hack

Talk to any avid gamer these days and they ll tell you about Lizard Squad.

This particular hacking group has been waging seemingly random attacks on the video game industry since the summer. They say they are doing it just because they can, and are both despised and revered by hundreds of thousands of people because of it.

Lizard Squad even sells T-shirts. Welcome to the 21st century, where hacking and other forms of digital disruption are entertainment, and hacker groups have fandoms.

And now, at least one security firm is tying Lizard Squad to the Sony hack.

Earlier this week, Los Angeles cybersecurity firm IntelCrawler told Bloomberg that both Lizard Squad and Guardians of Peace, the unknown group that has taken credit for Sony, share the same hacking timelines and slang.

Whether or not it is true, many in the gaming community are convinced Lizard Squad is responsible for the Sony hack.

Lizard Squad burst onto the scene on Aug. 18, when they claimed credit for server outages for the games League of Legends and Runescape. On the same day, the group threatened to take down the servers for the video game

company Riot Games and then proceeded to take down random players' channels on Twitch.tv, the live streaming service for gamers.

The nebulous group was able to take these servers down through a DDoS, or distributed denial of service, attack in which it directed Internet traffic to overwhelm its targets' servers. Less than a week later, Lizard Squad made headlines when it tweeted a fake bomb threat to American Airlines and successfully grounded the plane. Sony Online Entertainment president John Smedley was on the flight.

The bomb threat earned Lizard Squad infamy and thousands of Twitter followers. That same morning, Sony s Playstation Network was the target of a DDoS attack - Lizard Squad took credit.

To date, Lizard Squad has taken down (or claimed responsibility for) server outages of the games GTA 5, Destiny, Doda, League of Legends, Call of Duty, and Runescape, among others. Microsoft s XBox Live and Sony s Playstation Network have been attacked multiple times, as has Twitch.tv, along with various streamers on the site.

One streamer who was the target of Lizard Squad s shenanigans found his Twitch.tv chatroom swarmed with viewers that would donate to his channel with his own credit card, effectively donating his own money to himself. They ve also hacked into various gamer s computers, including relatively popular YouTube gamer Nick Sampson s desktop, leaving him the message lizards allow you to play for 1 hour then you must pay $30 amazon earlier this month.

Before their second Twitter account was suspended, Lizard Squad amassed more than 167,000 followers. They have a page on Know Your Meme, a website that chronicles top online phenomenon. Perusing the Lizard Squad public chat room while it was up revealed fans begging Lizard Squad to DDoS their high schools. Kids have sent Lizard Squad fan art while others have tweeted pictures with Lizard Squad written on their forehead, or just photos of themselves admitting to being overpowered by them.

On YouTube, searching Lizard Squad yields 42,900 results, beating the 19,200 videos referencing LulzSec, the comparable in popularity hacker group from 2011. (Note how Lizard Squad shares the same initials as LulzSec and the Lizard Squad original Twitter account was created at the same time as LulzSec s).

Lizard Squad is unlike any other hacking group primarily because of their relatively underground popularity. According to the social media monitoring service Topsy, Lizard Squad has been mentioned 86,000 times on Twitter in the past month, not counting retweets.

Hacker groups that have come before typically attack sites far-removed from people s everyday lives. Lizard Squad is different. It is going after something that young people use daily, something they love: their video games. Unlike LulzSec, Lizard Squad s work affects ordinary people, by disrupting their entertainment.

This disruption has upset many gamers. Mentions of Lizard Squad on Tumblr are almost entirely negative. Even some affiliates of the hacktivist collective Anonymous are incensed, with one releasing a video declaring war on them (Anonymous as a whole, however, seems amused by them).

Encouraged by anti-Lizard Squad sentiment, a small group calling themselves Finest Squad succeeded in getting Lizard Squad s Twitter

account suspended by filling out Twitter abuse forms. Finest Squad also claimed to have doxed Lizard Squad members, which is when adversaries go after targets online by dumping personal or sensitive information about them on the Web. But it turned out that much, if not all, of the personal information on Lizard Squad members turned out to be false.

Recently, Lizard Squad made various threats to take down XBox Live on Christmas Day, even after some of their members were allegedly arrested. Members deny that is the case.

So, why would Lizard Squad do this? Theories range from because we can or for the lulz, which comes from the online acronym LOL.

In multiple interviews with a YouTube personality known as Keemstar, Lizard Squad claims the bulk of their attacks are paid for, but these paid attacks are never announced on their Twitter feed as they are professionals and don t want to draw attention to their clients.

They call themselves DDoS for hire, and say they provide this service quite often. Paying someone to DDoS isn t a foreign concept in the video game community, and as a practice, has been going on for years. Gamers have been known to use this practice to knockout opponents in competitive matches.

For mayhem or profit, love them or hate them, the kids these days can t stop talking about Lizard Squad.

Microsoft Xbox Live Back Up, Sony PlayStation Network Still Down

Microsoft Corp’s Xbox Live was back up on Friday while Sony Corp’s PlayStation Network remained offline for a second day after a hacker group claimed responsibility for attacking the two Internet gaming services.

Gamers on Xbox Live and PlayStation Network experienced connection problems and delays on Christmas Day, one of the busiest times of the year for the video game industry. The majority of game and console sales are generated during the end-year holiday shopping season.

A message on PlayStation Network’s website on Friday read: "Under Scheduled Maintenance. We should be back online shortly. Apologies for any inconvenience." It directed users to the PlayStation blog and other related websites.

A Microsoft website that keeps track of the status of Xbox services listed Xbox Live’s "core services" as up and running on Friday. Several third-party apps on the platform were experiencing limited services, however.

A hacking group called "Lizard Squad" took credit for the disruption to both Xbox Live and PlayStation Network on Thursday. The group appeared unrelated to the "Guardians of Peace" hackers who broke into Sony Pictures’ network earlier this month to try to stop the release of the film "The Interview," which depicts the assassination of North Korean leader Kim Jong Un.

"The Interview" was released online on Wednesday on the Xbox network and other digital platforms. The movie also hit select U.S. theaters on

Thursday.

Lizard Squad: Kim Dotcom Plays Christmas Hero After Gaming Attacks

Call it a belated Christmas season miracle.

This is a story of an eccentric Internet entrepreneur who singlehandedly may have managed to save gamers around the world - and the Christmas season - from a hacking collective known as Lizard Squad.

Microsoft’s Xbox Live and Sony’s PlayStation Network both suffered outages Christmas Day that extended into today, frustrating gamers who were unable to enjoy their consoles for the holiday.

It seems all it took for Lizard Squad to call off the attacks the group said it perpetrated on the gaming networks was a little diplomacy from MegaUpload founder Kim Dotcom, according to Dotcom and Lizard Squad tweets.

The multimillionaire, who is based in New Zealand, is embattled in his own legal woes. He is expected to find out early next year whether he’ll be extradited to the United States, where he is wanted on charges related to piracy, copyright infringement and racketeering.

(Dotcom, who changed him name from Kim Schmitz, has said he is not guilty.)

Under the deal Lizard Squad said it reached with Dotcom, the group received 3,000 premium MegaPrivacy vouchers from Dotcom’s company, which allows it end-to-end encryption and secure storage services.

While it appeared both networks were still dark this morning, Lizard Squad tweeted it had stopped its "distributed denial of service attacks and said the current downtime is "just the aftermath."

Neither Microsoft nor Sony blamed the problem on hackers. Both companies said they were investigating the problems.

Cole Stryker, who explored the hacking culture in his book "Hacking the Future: Privacy, Identity, and Anonymity on the Web," said Lizard Squad’s style of hacking seems very similar to the "early days of LulzSec," a former hacking group.

"Very trollish, prankstery," Stryker told ABC News earlier this year. "I don t believe this person genuinely wants to be involved in geopolitics. I think this person is just having a laugh."

Still, the DDoS (distributed denial of service attacks) for which Lizard Squad has claimed credit has caused plenty of inconveniences.

Earlier this month, the group said it hacked Sony’s PlayStation Store.

Lizard Squad previously claimed responsibility for cyberattacks that briefly knocked the Vatican’s website, Battle.net and League of Legends offline.

Happy 35th Birthday, Gaming PC

35 years ago, a video game revolution was sweeping through American culture. Shopping mall arcades were crammed with teenagers blasting menacing Space Invaders and lethal Asteroids to fading phosphorous particles. Cartridge-based home gaming consoles were beginning to catch on, bringing interactive entertainment into living rooms. University computer labs intended for scientific research were overrun with students programming their own electronic versions of Dungeons & Dragons. And with the coming of the 1979 Christmas shopping season, two revolutionary new home computers from Atari appeared on store shelves, machines which would forever change our perceptions of what PCs were capable of.

Computers had broken into the home market two years before with the release of the Apple II, Radio Shack TRS-80, and Commodore PET. All three were stunningly primitive by contemporary standards, but they were real, affordable PCs priced just within the means of ordinary consumers. Thousands of people rushed out to purchase these technological wonderments, enchanted by the novelty of owning a piece of the future.

The problem was, computer owners weren t all that sure what they could actually do with the new silicon-powered toys. Commercial software was scarce and primitive. Many early home computer hobbyists programmed their own applications from scratch, learning BASIC as they pecked away and created home finance and cookbook databases. The more ambitious among these tinkerers tried their hand at creating their own video games.

Programming games on these hardware-limited machines required intense skill. Though Apple II creator Steve Wozniak famously ported his arcade game, Breakout, to the Apple II computer, few early developers could match Woz s technical mastery. Early PCs had more in common with calculators than gaming consoles, with hardware better suited to displaying text than animation. The arcane and memory-strapped nature of these early computers made game design a test of both innovation and endurance.

In the late 1970s, Atari was the largest and best-known manufacturer of video games in the world. Already successful in both the arcade and home gaming markets, they were eager to expand into the new frontier of home computing. As an established manufacturer of video game hardware, Atari approached their personal computer project very differently than their competitors. Atari PCs would be capable of word processing and data management, but the Atari logo was synonymous with great gaming, and that meant Atari s computer line would be expected to deliver the highest-quality entertainment experience on the market.

Atari s engineers decided that their home computers would be built around a standard core processor, then supplemented with custom graphics chips created just for playing games, a radical concept in personal computing. Their first PCs were built around the same 6502 eight-bit processor utilized by the Apple II, but clocked to a greater speed. Two specialized graphics coprocessors were then added, allowing the Atari to easily generate hardware-assisted sprites, play fields, and a broad color palette. A third special chip provided extra hardware functions for controller support and four dedicated sound channels for creating complex music and sound effects.

Atari created two versions of the new computer, dubbed the Atari 400 and Atari 800. The two models were fundamentally the same inside, but the 400 skewed toward the bargain end of the market thanks to a cheap membrane keyboard and a few other cost-cutting measures. Both models included the same special graphics and sound chips, as well as four controller ports for multiplayer games. The 400 and 800 could use cassette tape and floppy disk drives, but also included an input to run programs from a standard console-style ROM cartridge, an allowance which meant gamers wouldn t have to endure the painfully slow loading times then associated with computers.

When the 400 and 800 were released, they were far and away the most powerful home gaming machines available. The two computers were harbingers to the bleeding-edge technical advantage and cost which would thereafter characterize PC gaming. While more expensive than contemporary home consoles, they were also much more capable and expandable. The multi-colored, plentiful sprites generated by Atari s new computers looked like something from another planet, and the four-channel sound was unparalleled, allowing for superb sound and real musical accompaniment.

Arcade ports boasted tremendous fidelity, a terrific advantage in an era when arcade games were the technological gold standard for game design. Programmers quickly discovered ways to leverage the hardware toward better gaming. The ability to incorporate both a joystick and keyboard as controls led to complex, innovative new simulation games. Atari s first-party Star Raiders forced a player to balance reflexes and resources in a fast-paced strategic shooter. The Atari s four controller ports inspired multiplayer pioneer Dani Bunton to create the innovative and influential M.U.L.E, a fascinating and brilliant combination of cooperative and competitive game play. And Lucasfilm Games harnessed the Atari PC s capabilities in some of their earliest work, including the extraordinary exploratory shooter Rescue on Fractalus. The hardware was so ahead of its time that a homebrew programmer successfully ported Sega’s arcade classic Space Harrier to the platform in the early 21st century.

The multi-channel sound chip was also light-years ahead of the competition. Engineers harnessed up to four simultaneous instruments to duplicate popular musical themes and create original compositions. The chip also allowed complex, layered sound effects which granted games a special audial richness, a capability unparalleled until the introduction of the famous Commodore SID chip several years later.

Unfortunately, Atari unwisely choose to keep the deeper workings of their new computers secret. In an effort to maintain control over software distribution, they refused to release details of their powerful graphics hardware to hobbyist developers. This arbitrary barrier drove many creators away from the 400 and 800 and toward the much more open Apple II design. The Apple may have been less powerful, but its well-documented architecture made it far more accessible to a generation of garage programmers. Later competition from Commodore VIC-20 and 64 models further depressed Atari s market share. By the time Atari realized the mistake, it was too late, and fortune had passed them by. While Atari computers would remain relevant for a decade, they would never achieve the kind of PC industry dominance their initial technological advantage might have allowed.

Still, we contemporary gamers owe a great deal to the Atari 400 and 800. The graphics and sound chips designed for these computers were

forerunners of the graphics accelerators and dedicated audio hardware which are now standard equipment in gaming PCs. Atari s first computers helped launch a graphical arms race which would continue from the late seventies through today, a focus on increasingly-impressive GPU capabilities which would eventually inform the designs of the graphics processors powering both our PCs and the current generation of home consoles.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Stuck in Your New Game? Here s Where to Go for Help

You ve opened your presents. Now it s time to play with them.

With no responsibilities, a new stack of games, and the pizza delivery guy standing at the ready, you re all set to become a gaming hermit. But that nirvana can be shattered if you ve hit a puzzle or mission that proves too tough to pass.

While you could go to the nearest bookstore and grab a strategy guide, that would require spending money and, worse, putting on pants. Luckily, online gaming advice is cheap and plentiful.

Looking for help? If you re playing any of the following hot new games, here s where to look:

Dragon Age: Inquisition. Part of the problem with game guides is that they tend to spoil the story in their well-intentioned effort to help you out of a jam. IGN s walkthrough of our Game of the Year goes out of its way to avoid that as much as possible.

Dragon Age: Inquisition is so massive in scope that finding help could be a bit more difficult than usual, though. You may have to try several avenues to get the answer if you re on one of the many branching story arcs. But IGN s wiki is one of the most complete we ve come across, with details on everything from crafting to collectibles to which characters you can and can t have romances with.

Super Smash Bros. Super Smash Bros. is known for being pretty straightforward in its controls. But if you re picking it up for the first time, it s really easy to get lost or overwhelmed since the game lacks a tutorial mode and doesn t come with a comprehensive manual (and button mashing will get you only so far).

One suggestion is to spend some time on Twitch, watching experts play. That will show you what s possible, though you won t always learn how to do it yourself. To learn more, GameFAQs has a pretty good user-created repository full of tips, cheat codes, and level maps to make you more competitive.

Middle-earth: Shadow of Mordor. Prima is largely in the business of selling game guides, but if you re looking for broad-based advice rather than a specific solution to an in-game problem, the site has a wealth of tips for both beginners and advanced Mordor players. Some of that advice is pretty obvious, but other tips will let you navigate the game in a much easier fashion.

Call of Duty: Advanced Warfare. For the past few years, Activision has made it easy to thrive in the Call of Duty game with Call of Duty: Elite, a free service that let you review your stats and even suggested weapons to optimize your gameplay. Earlier this year, though, the publisher took it offline.

It didn t leave fans completely out in the cold, though. The Call of Duty: Advanced Warfare Companion app, available for iOS, Windows Phone, and Android devices, lets you create and manage a clan while you re on the go. It won t improve your aim, but it could get you some support to help you die a bit less in multiplayer matches.

Destiny. Destiny has been out longer than most games on this list, so there s been plenty of time for people to put together extensive walkthrough videos on YouTube and for the community to suss out which of those are the most helpful.

The quickest way to get that help is to know the level you re playing, as there are individual videos for each level online. Drop in, watch the player take care of the problem, and then drop out and try to emulate that yourself.

Far Cry 4. Taming Nepal isn t an easy task, especially in this epic quest. Gamers Heroes offers a thorough walkthrough of the game that will usher you through not only the main missions, but help you out with crafting, hunting, weapons, and how to conquer the game s various fortresses. You ll even learn how to get a quick Karma increase.

Prefer to take the shortcut and want to use cheat codes? Cheat Code Central has you covered, with exact coordinates of quest items and the locations of masks and propaganda posts, along with easy ways to boost your achievements.

The 5 Worst Video Games of 2014

It was the best of times, it was the worst of times.

Actually, when it comes to these five games, it was just the worst of times.

What happened? No one really sets out to make a terrible game. But bad design, buggy graphics, and broken gameplay happen anyway, and they happened in a big way to the following thumb-crushing disasters.

1. Dungeon Keeper (iOS) For 50 gems, I ll tell you why Dungeon Keeper, the penny-pinching mobile remake of a beloved 17-year-old strategy game, is bad news. You can get five gems for 10 gold coins, by the way, and if you click here you can buy packs of gold coins for $4.99 apiece. Or you could just go play the game, though you ll need some Red Jewels if you want to take more than five turns per day. Those cost 12 gems apiece.

Remember when you could just download and play a video game? By the way, that memory costs 100 Black Pearls. Do you have your credit card handy?

2. Sonic Boom: Rise of Lyric (Wii U) Pity poor Sonic. Instead of letting the overworked mascot enjoy his retirement, Sega keeps sticking him in bad games. This year they really outdid themselves. His latest disaster, Sonic Boom: Rise of Lyric, is part of an all-out media blitz that includes a TV show, comics, a toy line, and, yep, games. Spreading yourself thin is never a great way to make a good video game, and Rise of Lyric, with its broken, buggy platforming, repetitive action, and irritating characters, is not a good video game.

3. SoulCalibur: Lost Swords (PS3) The swords aren t the only things Bandai Namco lost while making this lousy fighter. They also lost the point of SoulCalibur, one of the greatest fighting franchises ever, by shamelessly converting it into a microtransaction-heavy, free-to-play mess with massive load times and zero multiplayer. Our souls are weeping.

4. Rambo: The Video Game (Xbox 360, PS3, PC) Remember Ikari Warriors? It was an old-school coin-op game that had a cool little rotating joystick and two-player support and pretty much let you rampage around as a wannabe Rambo. This new game is totally different, mostly in that it s terrible. Presumably funded via tickets won at a skee-ball machine, this unstable shooter takes you through memorable scenes from the three Rambo films by gluing you to a rail and making you blast anything that moves. We d be angry too, Rambo.

5. Escape Dead Island (Xbox 60, PS3, PC) Challenge accepted! Although really, we d just like to escape playing this brain-dead zombie game. It s infested with bugs, for one thing, though worse is the game s combo of boring action and impossibly steep difficulty. Actually, the interminable fetch quests are worse. No, wait, the glitchy graphics. We can t decide. Escape!

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

No, North Korea Didn t Hack Sony

The FBI and the President may claim that the Hermit Kingdom is to blame for the most high-profile network breach in forever. But almost all signs point in another direction.

So, The Interview is to be released after all.

The news that the satirical movie which revolves around a plot to murder Kim Jong-Un will have a Christmas Day release as planned, will prompt renewed scrutiny of whether, as the US authorities have officially claimed, the cyber attack on Sony really was the work of an elite group

of North Korean government hackers.

All the evidence leads me to believe that the great Sony Pictures hack of 2014 is far more likely to be the work of one disgruntled employee facing a pink slip.

I may be biased, but, as the director of security operations for DEF CON, the world s largest hacker conference, and the principal security researcher for the world’s leading mobile security company, Cloudflare, I think I am worth hearing out.

The FBI was very clear in its press release about who it believed was responsible for the attack: The FBI now has enough information to conclude that the North Korean government is responsible for these actions, they said in their December 19 statement, before adding, the need to protect sensitive sources and methods precludes us from sharing all of this information .

With that disclaimer in mind, let s look at the evidence that the FBI are able to tell us about.

The first piece of evidence described in the FBI bulletin refers to the malware found while examining the Sony Picture s network after the hack.

 Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.

So, malware found in the course of investigating the Sony hack bears strong similarities to malware found in other attacks attributed to North Korea.

This may be the case but it is not remotely plausible evidence that this attack was therefore orchestrated by North Korea.

The FBI is likely referring to two pieces of malware in particular, Shamoon, which targeted companies in the oil and energy sectors and was discovered in August 2012, and DarkSeoul, which on June 25, 2013, hit South Korea (it was the 63rd anniversary of the start of the Korean War).

Even if these prior attacks were co-ordinated by North Korea and plenty of security experts including me doubt that the fact that the same piece of malware appeared in the Sony hack is far from being convincing evidence that the same hackers were responsible. The source code for the original Shamoon malware is widely known to have leaked. Just because two pieces of malware share a common ancestry, it obviously does not mean they share a common operator. Increasingly, criminals actually lease their malware from a group that guarantees their malware against detection. Banking malware and certain crimeware kits have been using this model for years.

So the first bit of evidence is weak.

But the second bit of evidence given by the FBI is even more flimsy:

 The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example,

the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.

What they are saying is that the Internet addresses found after the Sony Picture attack are known addresses that had previously been used by North Korea in other cyberattacks.

To cyber security experts, the naivety of this statement beggars belief. Note to the FBI: Just because a system with a particular IP address was used for cybercrime doesn t mean that from now on every time you see that IP address you can link it to cybercrime. Plus, while sometimes IPs can be permanent , at other times IPs last just a few seconds.

 It isn t the IP address that the FBI should be paying attention to. Rather it s the server or service that s behind it.

As with much of this investigation our information is somewhat limited. The FBI haven t released all the evidence, so we have to go by what information is available publicly. Perhaps the most interesting and indeed relevant of this is the C2 (or Command and Control) addresses found in the malware. These addresses were used by whoever carried out the attack to control the malware and can be found in the malware code itself. They are:

* 202.131.222.102 Thailand
* 217.96.33.164 Poland
* 88.53.215.64 Italy
* 200.87.126.116 Bolivia
* 58.185.154.99 Singapore
* 212.31.102.100 Cyprus
* 208.105.226.235 USA

Taking a look at these addresses we find that all but one of them are public proxies. Furthermore, checking online IP reputation services reveals that they have been used by malware operators in the past. This isn t in the least bit surprising: in order to avoid attribution cybercriminals routinely use things like proxies to conceal their connections. No sign of any North Koreans, just lots of common, or garden, internet cybercriminals.

It is this piece of evidence freely available to anyone with an enquiring mind and a modicum of cyber security experience which I believe that the FBI is so cryptically referring to when they talk about additional evidence they can t reveal without compromising national security .

Essentially, we are being left in a position where we are expected to just take agency promises at face value. In the current climate, that is a big ask.

If we turn the debate around, and look at some evidence that the North Koreans might NOT be behind the Sony hack, the picture looks significantly clearer.

1. First of all, there is the fact that the attackers only brought up the anti-North Korean bias of The Interview after the media did the film was never mentioned by the hackers right at the start of their campaign. In fact, it was only after a few people started speculating in the media that this and the communication from North Korea might be linked that

suddenly it did get linked. My view is that the attackers saw this as an opportunity for lulz , and a way to misdirect everyone. (And wouldn t you know it? The hackers are now saying it s okay for Sony to release the movie, after all.) If everyone believes it s a nation state, then the criminal investigation will likely die. It s the perfect smokescreen.

2. The hackers dumped the data. Would a state with a keen understanding of the power of propaganda be so willing to just throw away such a trove of information? The mass dump suggests that whoever did this, their primary motivation was to embarrass Sony Pictures. They wanted to humiliate the company, pure and simple.

3. Blaming North Korea offers an easy way out for the many, many people who allowed this debacle to happen; from Sony Pictures management through to the security team that were defending Sony Picture s network.

4. You don t need to be a conspiracy theorist to see that blaming North Korea is quite convenient for the FBI and the current U.S. administration. It s the perfect excuse to push through whatever new, strong, cyber-laws they feel are appropriate, safe in the knowledge that an outraged public is fairly likely to support them.

5. Hard-coded paths and passwords in the malware make it clear that whoever wrote the code had extensive knowledge of Sony s internal architecture and access to key passwords. While it s (just) plausible that a North Korean elite cyber unit could have built up this knowledge over time and then used it to make the malware, Occam s razor suggests the simpler explanation of a pissed-off insider. Combine that with the details of several layoffs that Sony was planning and you don t have to stretch the imagination too far to consider that a disgruntled Sony employee might be at the heart of it all.

I am no fan of the North Korean regime. However I believe that calling out a foreign nation over a cybercrime of this magnitude should never have been undertaken on such weak evidence.

The evidence used to attribute a nation state in such a case should be solid enough that it would be both admissible and effective in a court of law. As it stands, I do not believe we are anywhere close to meeting that standard.

North Korea’s Internet Collapses After Sony Hack

North Korea’s Internet went dark for several hours amid rumors of US retaliation over its alleged hacking of a Hollywood studio, just as the pariah state came under attack at the UN over its rights record.

It was not clear who or what had shut down Pyongyang’s web connections, but cyber experts said the country’s already limited Internet went completely offline overnight from Monday to Tuesday local time.

Piling further pressure on Kim Jong-Un’s regime, UN members debated North Korea’s brutal treatment of its huge prison population after China, its only major ally, was rebuffed in a bid to shelve the issue.

US-based Internet analysts Dyn Research said Pyongyang’s four online networks, all connected through Chinese telecom provider China Unicom,

had been offline for nine hours and 31 minutes before services resumed on Tuesday morning.

Dyn Research said Pyongyang’s very limited infrastructure could be vulnerable to power outages but the way it had collapsed "seems consistent with a fragile network under external attack".

US President Barack Obama and the FBI have accused North Korea of being behind the hacking of Sony Pictures, which decided to cancel the Christmas Day release of comedy film "The Interview".

Washington officials refused to comment on speculation that the North Korean Internet blackout was the first stage in what Obama has warned will be a "proportionate response" to the hack.

North Korea has angrily insisted that it had nothing to do with the theft and leaking of Sony company secrets nor threats against moviegoers, but it has also condemned Sony’s madcap movie, which features a fictional plot to kill Kim.

Pyongyang has also vowed reprisals if the US brings in new sanctions such as restoring the country to a list of state sponsors of terrorism.

China on Tuesday suggested Washington and Pyongyang hold talks over cyber hacking. US officials, however, have dismissed a North Korean proposal for a joint investigation into the Sony hack and instead called for the hermit state to compensate the film studio.

Dyn Research said earlier Monday that Internet connectivity between North Korea and the outside world, never good at the best of times, had begun to show signs of instability over the weekend.

"This is different from short duration outages we have seen in the past," Earl Zmijewski, vice president of data analytics at Dyn, told AFP.

But Zmijewski stressed it was impossible to say what had caused the outage. "They could have elected to simply pull the plug or they could have suffered from some sort of failure or attack," he said.

The diplomatic row comes as China failed on Monday to block the first-ever UN Security Council meeting on North Korea’s dismal rights record after a strong majority of members voted in favor of it.

US ambassador Samantha Power - backed by envoys from Britain, Australia and France - said North Korean citizens experience a "living nightmare" of political repression.

She recalled testimony from a starving prison camp survivor who picked kernels of corn from cattle dung to eat and of a former guard who said prison wardens routinely raped prisoners.

Power dismissed Pyongyang’s offer of a joint investigation into the hack as "absurd," urging the council to take action against North Korean leaders.

No decision was taken on Monday on a call to refer North Korea to the International Criminal Court for crimes against humanity, but campaigners urged the body to keep the issue alive.

Beijing - which has itself been accused by Washington of extensive

hacking of civilian and government networks - meanwhile suggested on Tuesday that "the US and the DPRK can have communication" on cyber hacking, using North Korea’s official title.

Washington has urged Beijing, Pyongyang’s closest ally, to help rein in the North’s cyber crime activities, with US Secretary of State John Kerry speaking with his Chinese counterpart over the weekend to discuss the problem.

China’s foreign ministry on Monday condemned "cyber terrorism" in any form but did not refer directly to North Korea.

Elsewhere, Seoul heightened its readiness against cyber attacks from North Korean and other hackers after a series of online information leaks about the country’s nuclear power plants.

North Korea has limited access to the worldwide web with just four networks on the global Internet, compared to 150,000 in the United States, analysts say.

Pyongyang’s main Internet presence is through its Uriminzokkiri website, which has Twitter and Flickr feeds and is best known for posting propaganda videos excoriating South Korea and the United States.

U.S. Police Struggle To Uncover Threats on Social Media

U.S. law enforcement agencies are a long way from being able to effectively track threats of the kind a gunman posted on Instagram before his execution-style murder of two New York City policemen last weekend.

Police need more data analytics and mining software to monitor social media sites such as Facebook and Twitter , as well as trained personnel to make sense of what could be a deluge of data, say law enforcement officials and security experts.

"You can buy all the technology you want, but if you want to figure out clever stuff, you better have smart people able to use it," said Christopher Ahlberg, co-founder of Recorded Future Inc, which helps clients analyze social media feeds. The company is partly backed by In-Q-Tel, a venture capital firm that serves U.S. intelligence agencies.

According to the New York Police Department, Ismaaiyl Brinsley posted anti-cop slurs on the Instagram photo-sharing site hours before walking up to two officers in a parked squad car in Brooklyn and shooting them dead on Saturday.

Baltimore police said they discovered the Instagram posts after Brinsley shot and wounded his girlfriend earlier that day. But the NYPD did not learn of the posts - which included a photograph of a silver handgun and the message "I’m Putting Wings On Pigs Today. They Take 1 Of Ours... Let’s Take 2 of Theirs" - until it was too late.

Monitoring social media for out-of-the-blue threats may be beyond the capabilities of most police forces including even the New York Police Department, which has a relatively extensive and aggressive intelligence operation, experts say.

Analysts at the New York and Los Angeles police departments routinely crawl through social media to keep tabs on individuals on their radar, such as gang members, or to prepare for high-profile events. But in an era of shrinking or stagnant budgets, buying high-end software and hiring trained data analysts can be costly.

Many police departments utilize fairly rudimentary tools. The NYPD uses common search engines, experts say. It is possible to program an algorithm to pick up threatening messages, but the sheer volume of data and the potential number of "false positives" would impede its effectiveness.

"It is like trying to take a sip from a fire hydrant," the non-profit Police Executive Research Forum said in a 2013 report.

In monitoring social media, most local police forces lag U.S. intelligence agencies, which despite their vast surveillance networks still struggle to prevent attacks such as the 2013 Boston Marathon bombing.

The National Security Agency had raw intercepts pointing to a person matching the 2009 "underwear bomber's" description, but failed to stop him from boarding a plane.

The Department of Homeland Security monitors about 100 social media sites, but there are restrictions that keep their agents from sharing all the information that they collect directly with local law enforcement.

Social media monitoring by police tends to be reactive: analysts hit the Internet when someone phones in a tip. Investigators use social networking sites to identify victims, look for witnesses and perpetrators, generate leads or search for evidence in the aftermath of a crime.

"Most of the stuff, honestly, we get is when people send it to us," said Los Angeles Police Department spokesman, Commander Andrew Smith.

That's not to say there have not been some successes. The LAPD, which employs around 40 people to monitor social media manually, uses software from a startup called PredPol Inc, which stands for predictive policing. The software analyzes LAPD and other internal police databases to identify crime-ridden areas and determine the best times to patrol.

PredPol marketing manager Benjamin Hoehn said crime dropped around 20 percent within 10 months of deploying the system in Modesto, California, in January.

The LAPD is also exploring the use of Geofeedia Inc, which incorporates user-location data as it crawls through sites from Twitter and Facebook to Google Inc's YouTube and Yahoo Inc's Flickr.

Sophisticated services provided by the likes of Palantir Technologies Inc, which aids intelligence agencies in counter-terrorism, can track a person's movements, identify anonymous messages from writing patterns, or establish an individual's daily routines based on social media activity, experts said.

Ahlberg said Recorded Future can predict areas where social unrest will erupt with a high degree of accuracy, based on online commentary and other data, offering a glimpse of what may be possible.

Rights organizations have criticized the increasing use of social media crawling by law enforcement as a potential violation of privacy. Others argue anything posted on social media is fair game.

"You can call it infringing on their Frist Amendment rights but these are the 21st century tools available," said ex-FBI agent Kenneth Springer, who runs investigations outfit Corporate Solutions Inc.

Dangerous NTP Hole Ruins Your Chrissy Lunch

Critical holes have been reported in the implementation of the network time protocol (NTP) that could allow unsophisticated attackers root access on servers.

System administrators may need to forego the Christmas beers and roasted beasts until they've updated NTP daemons running versions 4.2.8 and below.

The grinch bug was announced by the US Industrial Control Systems Emergency Response Team, which received news of the hole from Google security researchers.

"Exploitation of these vulnerabilities could allow an attacker to execute arbitrary code with the privileges of the ntpd process," the agency said in an advisory.

"An attacker with a low skill would be able to exploit these vulnerabilities.

"Exploits that target these vulnerabilities are publicly available."

Google's Neel Mehta and Stephen Roettger reported two serious and four "less-serious" bugs which were patched in 4.2.8 released 18 December.

These included weak default keys, weak random number generator seeds, and buffer overflows.

Admins should backup operational industrial control system configurations and test the patch prior to deployment, the computer emergency response team urged.

It's also advisable to harden systems by minimising network exposure, including by shoving remote devices and - where applicable - control system networks behind firewalls and into isolated zones.

The Worst Spammers of 2014

On the flip side of year s best lists at this point on the calendar, we also have year s worst rankings. Email anti-clutter tool Unroll.me has just released its 2014 SPAMMYs, showcasing the sites that were the largest spam email offenders this year.

Chances are, if you have an email account, you ll recognize some of these

names.

Congratulations are due to online deal and coupon service LivingSocial for having sent out 285 pain-in-our-neck emails on average per user, tops for this year. At honorable mention was competitor Groupon, a close second with 282 emails per subscriber.

Check out the rest of the SPAMMYs rankings below, which include the email services that received the most unsubscribe requests by Unroll.me s customers, and also a rating of the spammiest holidays by number of themed emails this year.

(Oh, and we also featured Unroll.me as one of the ways to keep email from ruining your life.)

Most spam emails sent:

LivingSocial: 285 emails sent on average per user
Groupon: 282 emails sent on average per user
Facebook: 263 emails sent on average per user
LinkedIn: 199 emails sent on average per user
Twitter: 117 emails sent on average per user
Amazon: 97 emails sent on average per user
Pinterest: 87 emails sent on average per user
Google: 62 emails sent on average per user
Google Plus: 62 emails sent on average per user
YouTube: 43 emails sent on average per user
Etsy: 29 emails sent on average per user
eBay: 27 emails sent on average per user
Tumblr: 23 emails sent on average per user
Yelp: 21 emails sent on average per user
TicketMaster: 21 emails sent on average per user

Most unsubscribe requests:

StumbleUpon: 51 percent unsubscribe rate
MoveOn.org: 48 percent unsubscribe rate
Jetsetter: 47 percent unsubscribe rate
Monster: 44 percent unsubscribe rate
SlideShare: 44 percent unsubscribe rate
Live Nation: 43 percent unsubscribe rate
Angie s List: 41 percent unsubscribe rate
Rent The Runway: 39 percent unsubscribe rate
GameStop: 39 percent unsubscribe rate
NoMoreRack: 39 percent unsubscribe rate
Travelocity: 39 percent unsubscribe rate
Ancestry: 39 percent unsubscribe rate
Sports Authority: 39 percent unsubscribe rate
ProFlowers: 39 percent unsubscribe rate
Care.com: 38 percent unsubscribe rate

Most holiday-related spam emails sent:

Cyber Monday: average of 25 emails per user
Black Friday: average of 22 emails per user
Veterans Day: average of 18 emails per user
Thanksgiving: average of 17 emails per user
Election Day: average of 17 emails per user
Halloween: average of 17 emails per user
Tax Day: average of 16 emails per user

Columbus Day: average of 16 emails per user
Valentine s Day: average of 15 emails per user
Ash Wednesday: average of 15 emails per user
Cinco de Mayo: average of 15 emails per user
Saint Patrick s Day: average of 15 emails per user
Good Friday: average of 14 emails per user
Presidents Day: average of 13 emails per user
Martin Luther King, Jr. Day: average of 13 emails per user

US Judge: Facebook Cannot Avoid Class Action Lawsuit Over Scanning Users' Private Messages for Advertising Purposes

A U.S. judge has given the green light to a class action lawsuit that alleges Facebook scans private messages to create targeted advertisements. The plaintiffs claim that the social networking website violated several state and federal statutes.

Facebook cannot avoid the class action suit against its practice of scanning private messages of users for advertising purposes, according to U.S. District Judge Phyllis Hamilton of California. The case is moving forward because the company "has not offered a sufficient explanation of how the challenged practice falls within the ordinary course of its business," the judge said.

Three plaintiffs to the suit filed in January allege that Facebook violated federal and state statutes by scanning users' private messages to create targeted ads. The plaintiffs also believe that the mention of a company in the messages resulted as a "like."

The plaintiffs add that Facebook's messaging service is meant as a private communication tool between users.

"Facebook's practice of scanning the content of these messages violates the federal Electronic Communications Privacy Act (ECPA also referred to as the Wiretap Act), as well as California's Invasion of Privacy Act (CIPA), and section 17200 of California's Business and Professions Code," the plaintiffs said.

Facebook's motion to dismiss the plaintiffs' Wiretap Act claim and the CIPA section 631 claim were denied by Judge Hamilton.

However, the social media company's motion to dismiss the plaintiffs' claims on section 632 of the CIPA and section 17200 of the California Business & Professions Code, also known as the Unfair Competition Law, was granted.

Facebook maintains that it is responsible for handling the content of private messages to ensure proper delivery. It is, therefore, free to intercept private messages.

Facebook also believes that scanning messages is part of its normal business practice. The company, however, claims that it stopped doing so in 2012. The case then, Facebook believes, should not move forward.

The court read Facebook's full terms of service and found that the language used in the service terms was vague. The court stated that the document fails to clarify whether users had indeed given their consent

for Facebook to scan private messages for advertising purposes.

The plaintiffs have all reasons to expect that their private messages remained private. The plaintiffs also argue that even though Facebook has stopped scanning messages, it may start again whenever the company wishes to.

Facebook is not the only company that has been taken to court by users over privacy violations. Other companies such as Yahoo!, Earthlink and Google have faced similar lawsuits.

Google’s Gmail service was found violating the Wiretap Act as the company automatically scanned Gmail messages as part of its targeted ad strategy. Google is currently appealing against the violation.

Internet Privacy Is A Fantasy, Will Merely Be A Fetish by 2025

If you re still holding out hope for the preservation of Internet privacy, you may need to adjust your ideals a bit. The future of online privacy is cloudy, and policymakers and technology innovators have a weighty task on their hands one they re likely to fumble. This is one of the overarching findings of a recent canvassing of more than 2,500 experts by Pew Research Center s Internet & American Life Project.

The Future of Privacy is a report from Pew forecasting whether policymakers and technology leaders will be able to create a secure, popularly accepted, and trusted privacy-rights infrastructure by 2025 that allows for business innovation and monetization while also offering individuals choices for protecting their personal information in easy-to-use formats.

About 55 percent of respondents said they don t think the above will actually happen, while the other 45 percent said they do think a satisfactory privacy infrastructure will be established in the next 10 years.

A shared sentiment from both sides of the table was that online life is inherently public, something that won t surprise anyone who s part of a social network or has kept up with news headlines in recent years. Pew highlighted this anonymous response: Privacy will be the new taboo and will not be appreciated or understood by upcoming generations.

The report listed a number of common ideas shared by respondents, including: privacy and security are foundational issues of the digital world, we are living in an unprecedented condition of ubiquitous surveillance, we need little more than personal convenience to be compelled to share our personal information, and privacy norms are always changing.

Another theme gleaned from the responses to Pew s canvassing is that an arms race of sorts is unfolding, one between privacy-protecting technology and privacy-penetrating technology. As Google Glass and attendant projects grow, the so-called Internet of Things becomes increasingly aware of literally everything, and as programmers begin jumping on algorithmic schemes to sift, curate, and predict the data, notions of privacy will be considered a fetish, according to an attorney at a major law firm.

The hotly anticipated Apple Watch may be another test for the protection of personal privacy in an increasingly technology-dependent age. Connecticut Attorney State General George Jepsen recently requested to meet with Apple CEO Tim Cook about how personal data collected by the Apple Watch will be protected.

Apple Pushes First Ever Automated Security Update to Mac Users

Apple Inc has pushed out its first-ever automated security update to Macintosh computers to help defend against newly identified bugs that security researchers have warned could enable hackers to gain remote control of machines.

The company pushed out the software on Monday to fix critical security vulnerabilities in a component of its OS X operating system called the network time protocol, or NTP, according to Apple spokesman Bill Evans. NTP is used for synchronizing clocks on computer systems.

The bugs were made public in security bulletins on Friday by the Department of Homeland Security and the Carnegie Mellon University Software Engineering Institute. Carnegie Mellon identified dozens of technology companies, including Apple, whose products might be vulnerable.

When Apple has released previous security patches, it has done so through its regular software update system, which typically requires user intervention.

The company decided to deliver the NTP bug fixes with its technology for automatically pushing out security updates, which Apple introduced two years ago but had never previously used, because it wanted to protect customers as quickly as possible due to the severity of the vulnerabilities, Evans said.

"The update is seamless," he said. "It doesn t even require a restart."

Apple does not know of any cases where vulnerable Mac computers were targeted by hackers looking to exploit the bugs, he added.

Get Better Search Results with Windows 10’s Universal Search Feature

As you may know, the Universal Search feature in Windows is designed to provide you with search results from both your computer and the internet. Ever since it first made its appearance in Windows Vista, the Universal Search feature has undergone a series of evolutionary steps to get where it is now in the upcoming release of Windows 10. While the Windows 10’s Universal Search feature is a work in progress, it shows promise and is worth a preliminary investigation. Let’s take a closer look at the changes in Universal Search leading up to Windows 10.

As you may remember, Microsoft began to make some very serious improvements with the Search feature in Windows Vista. To begin with, the Search was integrated right into the Start Menu instead of being a

separate application. To search, you clicked the Start button and then began typing the name of the file in a search box. As soon as you typed the first letter, the Search engine immediately began compiling a list of applications, folders, and documents that began with that letter and displayed them in a categorized list right on top of the Start Menu, which instantly converted itself into the search results pane. As you continued typing letters, the Search engine refined its list to match the letters that you typed.

The search results pane also included a Search Internet feature that appeared at the bottom of the results and was automatically preloaded with the term you searched for (Figure A). If you clicked Search Internet, Windows Vista would pass the search job on to MSN Search, which would immediately conduct a search and present the results in an Internet Explorer window.

Among the new Search features in Windows Vista was the ability to search the internet as well as your system’s files and folders.

Like its much maligned predecessor, Windows 7 also included a search tool that was an integrated right into the Start Menu, and it worked with similar alacrity. However, the Universal Search feature was buried away in a secondary window. At the bottom of the search results pane was a link titled See more results. When you clicked that link, a Windows Explorer window appeared and showed all of the same results. At the bottom of the window was a section titled "Search again in" that included a link titled Internet (Figure B). When you clicked that link, Internet Explorer would launch and display the results from the default search engine.

Windows 7’s Universal Search feature was a bit harder to find.

As you may know, Windows 8 has a great Universal Search feature. However, since the Search feature was sort of buried in the operating system’s convoluted user interface, it really didn’t get the attention that it deserved. To access it, you either simply begin typing when you’re on the Start Screen, or you access the Charms bar and then click the Search Charm. In Windows 8.1, a Search icon was added to the top right of the Start Screen. In any case, as soon as you start to type, the search results pane begins displaying results from your computer (files, folders, and programs) as well as results from the internet.

While the Search feature was difficult to access in Windows 8, the Universal Search results were readily apparent.

When you click a result from the internet, the results pane transforms into a great looking modern UI Results screen powered by Bing, which presents a multitude of results accompanied with detailed synopsis that you can read through to find what you’re looking for (Figure D). When you click on one of the items on this screen, Internet Explorer launches and takes you to that site.

The main Results screen in Windows 8 provides a beautiful and easy-to-use display.

In Windows 10, with the return of the Start Menu, you’ll once again find the search tool integrated right into the Start Menu. As soon as you begin typing, the Search engine immediately begins compiling a list of applications, folders, and documents. It also links to places on the internet that contain the term and displays them on the Start Menu

results pane.

At this point in time, the initial Windows 10 search results pane is pretty simple.

When you select a search term result from the internet, you'll see a modern UI results screen powered by Bing.

At this point in time, the main results pane in Windows looks a lot like Internet Explorer.

What's your take?

Like its recent predecessors, Windows 10 contains a Universal Search feature that provides you with search results from both your computer and the internet. Of course, Windows 10's Universal Search feature is still a work in progress, but it shows promise. Have you taken advantage of the Universal Search feature in previous versions of the Windows operating system? Do you think that you'll use it in Windows 10? Share your opinion in the discussion thread below.

HP Will Release A Revolutionary New Operating System in 2015

Hewlett-Packard will take a big step toward shaking up its own troubled business and the entire computing industry next year when it releases an operating system for an exotic new computer.

The company s research division is working to create a computer HP calls The Machine. It is meant to be the first of a new dynasty of computers that are much more energy-efficient and powerful than current products. HP aims to achieve its goals primarily by using a new kind of computer memory instead of the two types that computers use today. The current approach originated in the 1940s, and the need to shuttle data back and forth between the two types of memory limits performance.

 A model from the beginning of computing has been reflected in everything since, and it is holding us back, says Kirk Bresniker, chief architect for The Machine. The project is run inside HP Labs and accounts for three-quarters of the 200-person research staff. CEO Meg Whitman has expanded HP s research spending in support of the project, says Bresniker, though he would not disclose the amount.

The Machine is designed to compete with the servers that run corporate networks and the services of Internet companies such as Google and Facebook. Bresniker says elements of its design could one day be adapted for smaller devices, too.

HP must still make significant progress in both software and hardware to make its new computer a reality. In particular, the company needs to perfect a new form of computer memory based on an electronic component called a memristor.

A working prototype of The Machine should be ready by 2016, says Bresniker. However, he wants researchers and programmers to get familiar with how it will work well before then. His team aims to complete an operating system designed for The Machine, called Linux++, in June 2015. Software that emulates the hardware design of The Machine and other

tools will be released so that programmers can test their code against the new operating system. Linux++ is intended to ultimately be replaced by an operating system designed from scratch for The Machine, which HP calls Carbon.

Programmers experiments with Linux++ will help people understand the project and aid HP s progress, says Bresniker. He hopes to gain more clues about, for example, what types of software will benefit most from the new approach.

The main difference between The Machine and conventional computers is that HP s design will use a single kind of memory for both temporary and long-term data storage. Existing computers store their operating systems, programs, and files on either a hard disk drive or a flash drive. To run a program or load a document, data must be retrieved from the hard drive and loaded into a form of memory, called RAM, that is much faster but can t store data very densely or keep hold of it when the power is turned off.

HP plans to use a single kind of memory in the form of memristors for both long- and short-term data storage in The Machine. Not having to move data back and forth should deliver major power and time savings. Memristor memory also can retain data when powered off, should be faster than RAM, and promises to store more data than comparably sized hard drives today.

The Machine s design includes other novel features such as optical fiber instead of copper wiring for moving data around. HP s simulations suggest that a server built to The Machine s blueprint could be six times more powerful than an equivalent conventional design, while using just 1.25 percent of the energy and being around 10 percent the size.

HP s ideas are likely being closely watched by companies such as Google that rely on large numbers of computer servers and are eager for improvements in energy efficiency and computing power, says Umakishore Ramachandran, a professor at Georgia Tech. That said, a radical new design like that of The Machine will require new approaches to writing software, says Ramachandran.

There are other prospects for reinvention besides HP s technology. Companies such as Google and Facebook have shown themselves to be capable of refining server designs. And other new forms of memory, all with the potential to make large-scale cloud services more efficient, are being tested by researchers and nearing commercialization.

 Right now it s not clear what technology is going to become useful in a big way, says Steven Swanson, an associate professor at the University of California, San Diego, who researches large-scale computer systems.

HP may also face skepticism because it has fallen behind its own timetable for getting memristor memory to market. When the company began working to commercialize the components, together with semiconductor manufacturer Hynix, in 2010, the first products were predicted for 2013.

Today, Bresniker says the first working chips won t be sent to HP partners until 2016 at the earliest.

Dashlane s Password Manager Is Ultra-Convenient and Incredibly Smart

Despite seemingly constant security breaches on the Internet, people continue to use dumb passwords. Even one of the FBI s most wanted hackers used his cat s name (Chewy) to secure his accounts.

We use terrible passwords because they re otherwise hard to remember, and despite all the warnings and advice we hear, changing them is absurdly tedious. But a potential fix has arrived in the form of an updated password manager from the cybersecurity company Dashlane.

The desktop app, announced last week, can automatically organize and analyze your passwords across multiple services. It can also instantly change every single one of your passwords to secure and unique ones, without your having to visit a single site.

Though there s currently a bit of a wait list to access the tool, eventually anyone who wants in will be able to install the free software.

And once you see some of its best features I tried out below, you ll definitely want to.

When you log in to the Dashlane desktop app, it ll ask for access to your browser and then automatically recognize the passwords you ve already saved in your browser s password locker.

After waiting for a few moments, and granting the Dashlane app access to certain accounts, they ll appear before your eyes, like magic.

Analyze the quality of your passwords?After the system has your account information, you can navigate the app s sidebar to complete different tasks. Click on the Security Dashboard, and it automatically runs an analysis on your passwords and then gives you a score out of 100 percent, as shown below:

It identifies what your specific problems are whether it s weak passwords, compromised passwords, or reused passwords and then creates pathways for you to solve them. For instance, in the few passwords it collected from my accounts, it found that I repeat them often. So I was able to open up a list of the suspect security codes and change them. Which leads us to what is, quite possibly, Dashlane s best feature

Dashlane advertises that its Password Manager can change all your accounts security codes with just one click. In theory, this is possible. But in practice it s a little bit more complicated than that.

You can identify which accounts you want to change your password for manually, by selecting the Password section on the app s sidebar, or via a nifty tool like the one I mentioned above. It ll show you a list, and you can check a box to the right of each account you want to alter, like so:

Once you click the green Change passwords button in the upper-right corner of the screen, Dashlane will begin connecting with each separate website to do the deed. This is where it gets messier than Dashlane advertises.

Dashlane will connect to each website separately, assuming your account is still active and whatever login info you had saved in your browser

is up to date. In some cases, you may need to answer security questions you created on an individual website (What s your mother s maiden name?) to get Dashlane into a site. Those queries pop up in separate boxes and add some lag to the process.

When it s all done, each account will be assigned a new ultra-secure password: long strings of letters and numbers that you will never have to remember. All of these are securely encrypted locally on your computer. The only thing you need to remember to access them is your Dashlane account s master password (which is securely verified with a code sent to your email, every time you log in).

Eventually, Dashlane will let you tailor your account so that some passwords just automatically change themselves at set intervals. (In case you weren t aware, changing your passwords often is the main way you avoid getting hacked.)

After all this, you can download Dashlane s browser extension, available for Safari, Firefox, and Chrome.

Once it s installed and you ve logged in, a small Dashlane symbol of a jumping gazelle-like animal will appear in any username and password box you come across online.

Click the symbol, and all your login options will appear. If you have multiple logins for an account, Dashlane will show the varying usernames.

Once you select an account, it ll automatically log you in. In cases where you have only one account, it ll automatically enter the information and begin logging you in once you arrive at the sign-in page. (This setting is adjustable, in case you share your computer with someone.)

The only catch?While the password manager is free on your desktop (where I d guess most of us do our password changing), it ll sync to your mobile devices only if you sign up for a premium account, which costs $40 a year. This is more expensive than Dashlane s competitors like LastPass ($12 a year) and 1Password (a one-time $50 cost for Mac or Windows clients but free on mobile). Compared with those two, however, Dashlane is better designed and easier to use, and the auto-change feature is likely to make passwords more secure for its users than anything the competition offers right now.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial

media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.